

KEJAHATAN DEFECTING:

Studi Perbandingan antara

Undang-Undang ITE dan Hukum Pidana Islam

Ahmad Muyasir

Fakultas Syariah dan hukum Universitas Islam Negeri Sunan Kalijaga Yogyakarta
Jl. Marsda Adi Sucipto Yogyakarta. Email: ahmadmuyasir7@gmail.com

Abstract

As the technology advances, the crime is no longer just happening in the real world, but it is already reaching into the virtual world or virtual. In this case, defacing a form of cyber crimes is quite disturbing and has hurt many people. He is cybercrime is done by changing the look of the website of a website, either in part or seeluruhnya by firstly breaking into another person, without the owner's permission. This paper is going to examine the phenomenon of cyber crime (cyber crime), along with betuk, motives, consequences, and legal sanctions. In this paper, the problem of evil defecting will be assessed from the perspective of the Indonesian Criminal law and Islamic Criminal law (Fiqh Jinayah).

Seiring dengan berkembangnya teknologi, tindakan kejahatan tidak lagi hanya terjadi di dunia nyata, tetapi sudah merambah masuk ke dunia maya. Dalam hal ini, defacing merupakan salah satu bentuk kejahatan dunia maya yang cukup meresahkan dan telah merugikan banyak orang. Ia merupakan kejahatan mayantara yang dilakukan dengan cara mengubah tampilan website suatu website, baik sebagian ataupun seeluruhnya dengan cara terlebih dahulu menerobos sistem orang lain, tanpa izin pemiliknya. Tulisan ini hendak mengkaji feomena kejahatan dunia maya (cybercrime), beserta betuk, motif, akibat yang ditimbulkan, dan sanksi hukumnya. Dalam tulisan ini, masalah kejahatan defecting tersebut akan dikaji dari perspektif hukum Pidana Indonesia dan juga hukum Pidana Islam (Fiqh Jinayah).

Kata Kunci: *Kejahatan defecting*, Hukum Positif Indonesia, *Jarimah ta'zir*, Hukum pidana Islam

A. Pendahuluan

Dalam kehidupan ini, kemajuan teknologi merupakan sesuatu yang tidak bisa dihindari. Ia berjalan bersamaan dengan kemajuan peradaban, teknologi dan ilmu pengetahuan.¹ Teknologi membantu manusia dalam berinteraksi dengan manusia lain tanpa adanya batasan ruang dan waktu. Internet merupakan salah satu produk dari perkembangan teknologi.² Kemunculannya telah menyebabkan adanya perubahan pada struktur masyarakat menuju globalisme.³ Meskipun demikian, internet dengan segala kelebihanannya juga memiliki sisi kelemahan dan sering kali berdampak buruk jika dipergunakan oleh orang-orang yang tidak bertanggung jawab. Adanya *cyberspace* (ruang pada dunia maya) memberi peluang terjadinya kejahatan atau yang lebih dikenal dengan *cybercrime* (kejahatan dunia maya).

Pada umumnya, masyarakat Indonesia hanya akrab dengan istilah *hacking*, yaitu menerobos sistem orang lain tanpa izin, dan bahkan mereka beranggapan bahwa semua kejahatan dunia maya adalah *hacking*. Padahal banyak sekali bentuk-bentuk kejahatan dunia maya, dan salah satunya adalah *defecting*.⁴

Bagi sebagian besar masyarakat Indonesia, *defacing* barangkali masih menjadi sebuah kata yang terdengar ganjil. Akan tetapi bagi kalangan yang mendalami teknologi dalam ruang lingkup dunia maya, term *defacing* sebenarnya bukanlah kata yang asing. Ia yang merupakan salah satu bentuk kejahatan di dunia maya yang dilakukan dengan cara mengubah tampilan suatu *website*, baik halaman utama atau *index file* ataupun halaman lain yang masih terkait dalam satu *Uniform Resource Locator (URL)*⁵ di *website* tersebut

¹ Budi Agus Riswandi, *Hukum Internet di Indonesia*, (Yogyakarta: UII Press, 2003), hlm. 1.

² Abdul Wahid dan Mohammad Labib, *Kejahatan Mayantara (Cybercrime)*, (Jakarta: Refika Aditama, 2005), hlm. 103.

³ *Ibid.*

⁴ Dikdik M. Arief Mansur dan Elisatris Gultom, *Cyberlaw Aspek Hukum Teknologi Informasi*, Cet-II (Bandung: Refika Aditama, 2009), hlm. 4.

⁵ **URL** (*Uniform Resource Locator*) adalah rangkaian karakter menurut suatu format standar tertentu, yang digunakan untuk menunjukkan alamat suatu sumber,

(bisa di *folder* ataupun di *file*).⁶ Kejahatan *defacing* itu sendiri dilakukan dengan dua tahap, yaitu melakukan *hacking* terlebih dahulu ke dalam *web server* dan kemudian mengganti halaman *website* (*web page*).⁷

Untuk menjamin adanya kemaslahatan, keadilan, serta keseimbangan dan harmonisasi maka negara (pemerintah) memunculkan kebijakan yang berkaitan dengan tindakan kriminal, baik melalui kebijakan Penal (pemberantasan kejahatan dengan hukum pidana) maupun kebijakan non-Penal (pemberantasan kejahatan tanpa hukum pidana).⁸ Salah satu kebijakan Penal pemerintah dalam upaya memberantas *cybercrime* (kejahatan dunia maya) adalah dengan memunculkan Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (ITE) yang disahkan pada 21 April 2008.⁹ Undang-undang ini mencakup hal yang luas dan disesuaikan dengan kebutuhan saat ini.¹⁰

Dalam hukum Islam, persoalan tindak pidana dan hukuman terhadap para pelakunya dibahas dalam fiqh jinayah. Dalam fiqh jinayah, seseorang yang melakukan tindakan yang dilarang oleh *syara'* dikategorikan sebagai perbuatan *jarīmah*. Dalam hal ini, *jarīmah* diartikan sebagai larangan-larangan *syara'* yang diancam oleh Allah dengan hukuman *ḥad* (hukuman yang sudah ada ketentuannya dalam *nash* Al-Qur'an atau as-Sunnah) atau *ta'zīr* (hukuman yang tidak ada *nash*-nya).¹¹ Mengingat *defacing* merupakan tindak kejahatan yang relatif baru maka ia bisa dikategorikan sebagai *jarīmah ta'zīr*. Dalam hal ini, *defacing* tidak dapat diqiyāskan dengan *jarīmah ḥudūd* lain, tidak seperti *carding* (pembobolan kartu kredit) yang bisa diqiyāskan dengan pencurian. Hukum Islam tersebut mengatur dan menetapkan hukuman bagi para pelaku tindakan pidana dengan tujuan agar bisa memberi rasa jera serta guna menghentikan kejahatan sehingga bisa tercipta rasa aman dan tenteram dalam masyarakat.

seperti dokumen dan gambar di Internet. Lihat <http://id.wikipedia.org/wiki/URL>, diakses pada 4 Maret 2015 pukul 15.00 WIB.

⁶ Sutan Remi Syahdeini, *Kejahatan dan Tindak Pidana Komputer*, (Jakarta: Pustaka Utama Grafiti, 2009), hlm. 124.

⁷ *Ibid.*

⁸ Widodo, *Aspek Hukum Pidana Kejahatan Mayantara*, (Yogyakarta: Aswaja Pressindo, 2013), hlm. 179.

⁹ Sutan Reimy Syahdeini, *Kejahatan dan Tindak Pidana Komputer ...*, hlm. 225.

¹⁰ *Ibid.*

¹¹ Ahmad Hanafi, *Azaz-azaz Hukum Pidana Islam*, (Jakarta: Bulan Bintang, 2002), hlm. 121.

B. *Defacing* dan Posisinya dalam Ruang Lingkup *Cybercrime*

Seiring dengan berkembangnya teknologi, tindakan kejahatan tidak hanya terjadi di dunia nyata, tetapi sudah memasuki dunia maya atau virtual (*cyberspace*).¹² Hal ini terjadi karena kecanggihan teknologi telah membuka peluang bagi terjadinya kejahatan dunia maya. Kejahatan itu sendiri sering dipahami sebagai suatu tindakan yang melanggar undang-undang atau ketentuan yang berlaku dan diakui secara sah. Sementara dalam perspektif sosiologis, kejahatan merupakan suatu pola tingkah laku yang mendapat reaksi sosial dari masyarakat.¹³ Suatu tindakan bisa dikategorikan sebagai kejahatan adalah karena perbuatan tersebut bersifat merugikan atau merusak, baik menyangkut kepentingan individu maupun kepentingan kelompok atau masyarakat.

Munculnya internet di dunia modern telah melahirkan jenis kejahatan baru yang dinamakan *cybercrime* atau kejahatan dunia maya. Ada beragam definisi tentang *cybercrime*. Kepolisian Inggris, misalnya, mendefinisikan *cybercrime* sebagai segala macam penggunaan jaringan komputer untuk tujuan kriminal dan atau kriminal berteknologi tinggi dengan menyalahgunakan teknologi digital.¹⁴ Sementara Indra Safitri, sebagaimana dikutip oleh Achmad Tahir, mendefinisikan kejahatan dunia maya sebagai jenis kejahatan yang berkaitan dengan pemanfaatan sebuah teknologi tanpa batas serta memiliki karakteristik yang kuat dengan sebuah rekayasa teknologi yang mengandalkan pada tingkat keamanan yang tinggi dan kredibilitas dari sebuah informasi yang disampaikan dan diakses oleh pelanggan internet.¹⁵

Dalam *back ground paper* untuk lokakarya di kongres PBB x/2000 digunakan istilah CC untuk menunjuk pada kejahatan dunia maya atau *cybercrime* (lihat dokumen A/CONF.187/10). Dalam dokumen itu, sebagaimana dikutip oleh Ahmad Tahir, *cybercrime* dibedakan ke dalam dua kategori, yakni *cybercrime* dalam arti sempit dan *cybercrime* dalam arti luas.¹⁶ Adapun istilah yang digunakan untuk menunjuk *cybercrime* dalam

¹² Widodo, *Memerangi Cybercrime Karakteristik Motivasi dan Strategi Penanganannya dalam Perspektif Kriminologi*, (Yogyakarta: Aswaja Pressindo, 2013), hlm. 1.

¹³ Abdul Wahid dan Mohammad Labib, *Kejahatan Mayantara....*, hlm. 37.

¹⁴ *Ibid.*, hlm. 4.

¹⁵ Achmad Tahir, *Cybercrime: Akar Masalah, Solusi, dan Penanggulangannya*, (Yogyakarta: Suka Press, 2011), hlm. 34.

¹⁶ *Ibid.*, hlm. 35.

arti sempit adalah *computer crime*, sementara istilah yang digunakan untuk menunjuk *cybercrime* dalam arti luas adalah *computer related crime*.¹⁷

Dalam dokumen tersebut, *cybercrime* dalam arti sempit (*in a narrow sense*) didefinisikan sebagai *any legal behavior directed by means of electronic operations that target the security of computer system and the data processed by them* (setiap pelaku ilegal yang ditujukan pada operasi elektronik yang menargetkan sistem keamanan komputer dan data yang diproses oleh sistem komputer tersebut).¹⁸ Sementara *cybercrime* dalam arti luas (*in a broader sense*) didefinisikan sebagai *any legal behavior committed by means on in relation to, a computersystem or network, including such crime as illegal possession, offering or distributing information by means of a computer system or network* (setiap perilaku ilegal yang dilakukan dengan maksud atau berhubungan dengan sistem Komputer atau jaringan, termasuk kejahatan pemilikan, penawaran atau distribusi informasi dari sistem atau jaringan komputer).¹⁹

Kejahatan dunia maya (*cybercrime*) itu sendiri memiliki beragam tipe atau kategori. Ford dan Gordon, misalnya, sebagaimana dikutip oleh Faizin Sulistio, membagi jenis kejahatan mayantara atau kejahatan dunia maya menjadi dua kategori: *pertama*, kejahatan *cyber* yang berupa satu kali serangan terhadap seseorang, dan *kedua*, kejahatan *cyber* yang terjadi setelah terjadi adanya pengulangan atau interaksi beberapa kali antara pelaku dan korban.²⁰ Sementara itu, Dikdik M. Arief Mansur dan Elesatris Gultom dalam bukunya yang bertitel *Cyberlaw Aspek Hukum Teknologi Informasi*, menyebutkan beberapa bentuk kejahatan yang berhubungan dengan penggunaan teknologi informasi yang berbasis utama komputer dan jaringan telekomunikasi:²¹

1. *Unauthorized Access to Computer System and Service*, yaitu kejahatan yang dilakukan dengan memasuki atau menyusup ke dalam suatu sistem jaringan komputer secara tidak sah (tanpa izin atau

¹⁷ *Ibid.*

¹⁸ *Ibid.*

¹⁹ *Ibid.*

²⁰ Contoh dari kejahatan tipe pertama adalah *phising*, *theft* (pencurian), *or manipulation of data* (manipulasi data), *identity theft* (pencurian identitas), ataupun *e-commerce fraud* (penipuan *e-commerce*). Sedangkan contoh kejahatan tipe kedua adalah *cyberstalking*, *harassment*, *extortion stock market manipulation*. Lihat Faizin Sulistyo, *Hukum Pidana dalam Perspektif*, (Denpasar: Pustaka Larasan, 2012), hlm. 128.

²¹ Dikdik M. Arief Mansur dan Elesatris Gultom, *Cyberlaw Aspek Hukum Teknologi Informasi*, (Bandung: Refika Aditama, 2009), hlm. 9.

tanpa sepengetahuan dari pemilik sistem jaringan komputer yang dimasukinya).

2. *Illegal Contents*, yakni kejahatan dengan memasukkan data atau informasi ke internet tentang sesuatu hal yang tidak benar, tidak etis, dan dapat dianggap melanggar hukum atau mengganggu ketertiban umum. Sebagai contoh, pemuatan suatu berita bohong atau fitnah yang akan menghancurkan martabat atau harga diri pihak lain.
3. *Cyber Espionage*, yakni kejahatan yang memanfaatkan jaringan internet untuk melakukan kegiatan mata-mata terhadap pihak lain, dengan memasuki sistem jaringan komputer (*computer network system*) pihak sasaran.
4. *Cyber Sabotage and Extortion*, merupakan kejahatan yang dilakukan dengan membuat gangguan, perusakan dan penghancuran terhadap suatu data, program komputer atau sistem jaringan komputer yang tersambung dengan internet. Biasanya kejahatan ini dilakukan dengan menyusupkan suatu *logic bomb*,²² virus komputer ataupun suatu program tertentu, sehingga data, program komputer atau sistem jaringan komputer tidak dapat dijalankan sebagaimana mestinya. Dalam beberapa kasus terjadi pekaku kejahatan menawarkan diri kepada korban untuk memperbaikinya dengan bayaran tertentu.
5. *Offense against Intellectual Property*, yakni kejahatan yang umumnya ditujukan untuk melanggar hak atas kekayaan intelektual yang dimiliki pihak lain di internet. Sebagai contoh, peniruan tampilan pada *web page* suatu situs milik orang lain secara ilegal, penyiaran suatu informasi di internet yang ternyata merupakan rahasia dagang orang lain, dan sebagainya.
6. *Infringements of Privacy*. Kejahatan ini biasanya ditujukan terhadap keterangan pribadi seseorang yang tersimpan pada formulir data pribadi yang tersimpan secara *computerized* yang apabila diketahui oleh orang lain maka dapat merugikan korban secara materil maupun immateril, seperti nomor kartu kredit dan nomor PIN ATM.²³

²² *Logic bomb* adalah suatu program yang dibuat dan dapat digunakan sewaktu-waktu. Dari situ akan terlihat bahwa informasi yang ada dalam komputer tersebut dapat terganggu, rusak, atau bahkan hilang. Lihat Maskun, *Kejahatan Siber suatu Pengantar*, (Jakarta: Kencana, 2014), hlm. 53.

²³ *Ibid.*

Dari paparan di atas maka dapat disimpulkan bahwa *cybercrime* pada dasarnya meliputi semua tindak pidana yang berkenaan dengan informasi, sistem informasi itu sendiri, serta sistem komunikasi yang merupakan sarana untuk penyampaian atau pertukaran informasi kepada pihak lain.²⁴ Lantas, bagaimana *cybercrime* (kejahatan dunia maya) itu dilakukan?

Di dalam *cybercrime* terdapat istilah *hactivism*, yaitu aktivitas yang dilakukan oleh *hacker*.²⁵ Aktivitas kejahatan tersebut dilakukan dengan dua tahap: pertama-tama pelaku melakukan *hacking* (pembobolan sistem komputer)²⁶ dan setelah itu pelaku kemudian melakukan *activism*. Adapun *hactivism* sendiri berbeda dengan *cyberterrorism* sekalipun keduanya ada unsur kesamaannya (sama-sama dilakukan dengan terlebih dahulu melakukan *hacking*), tetapi berbeda dalam tujuan dan akibatnya. Jika *cyberterrorism* bertujuan, antara lain, menimbulkan ketakutan, maka *hactivism* sama sekali tidak menimbulkan ketakutan dan hanya bermaksud mencemooh korban. Jika dilihat dari sisi akibat yang ditimbulkan, maka *cyberterrorism* dapat mengakibatkan kerugian yang dahsyat kepada masyarakat, seperti merusak sistem informasi bank sentral, merusak jaringan listrik, dan merusak jaringan badan pengawas pasar modal, sedangkan *hactivism* paling jauh hanya mengubah tampilan situs atau *defacing* dan tidak menimbulkan korban jiwa atau kerusakan terhadap infrastruktur dan property masyarakat.

Hactivism itu sendiri memiliki beragam bentuk. Alexandra Whitney Samuel sebagaimana dikutip oleh Sutan Remi Syahdeini menyebutkan sembilan bentuk kejahatan komputer (*electronic mischief*), yaitu: (1) *Site Defacement/defacing* / pengubahan tampilan situs, (2) *Site Direct* / pembelokan situs, (3) *Denial of service attack* / serangan-serangan DOS, (4)

²⁴ *Ibid.*, hlm. 10.

²⁵ *Hecker* adalah sebutan bagi pelaku *hacking*.

²⁶ Selain *hacking*, dalam dunia komputer dan internet juga terdapat istilah *cracking*. Jika *hacking* adalah kegiatan menerobos program komputer milik orang/pihak lain, dan pelaku atau orang yang gemar *ngoprek* komputer, memiliki keahlian membuat dan membaca program tertentu dan terobsesi mengamati keamanan (*security*)-nya disebut *hacker*. Sedangkan *cracking* merupakan *hacking* untuk tujuan jahat, dan pelaku atau orang yang melakukan kejahatan tersebut dikenal dengan istilah *cracker*. Ia adalah *hacker* bertopi hitam (*black hat hacker*). Meski sama-sama menerobos keamanan komputer orang lain, *hacker* lebih fokus pada prosesnya, sedangkan *cracker* lebih fokus untuk menikmati hasilnya. Lihat Sutan Remy Sahdeini, *Kejahatan dan Tindak Pidana Komputer...*, hlm. 118-119.

Information theft / pencurian informasi, (5) *Information theft and distribution* / pencurian informasi dan pendistribusian informasi curian tersebut, (6) *Virtual sit-ins* / pendudukan situs, (7), *Site parody* / parody situs, (8) *Virtual sabotage* / sabotase virtual, dan (9) *Software development* / pengembangan perangkat lunak).²⁷

Dari paparan di atas tampak jelas bahwa terdapat berbagai macam *hactivism*, dan *defacing* hanyalah salah satu bentuk dari *hactivism* itu. *Defacing* merupakan aktivitas *modification*; dalam arti tindakan melakukan perubahan terhadap data atau informasi atau konten yang mengalir dalam sebuah infrastruktur teknologi informasi tanpa sepengetahuan yang mengirimkan atau menerimanya.²⁸

Kejahatan dunia maya atau *cybercrime* itu sendiri pada dasarnya banyak sekali jenisnya. Jika dilihat berdasarkan modus operandinya, maka *cybercrime* bisa dibedakan ke dalam beberapa bentuk: (1) Akses tidak sah / *illegal acces*, (2) Penyadapan tidak sah / *intercepting*, (3) Pengubahan data / *defacing*, (4) Penyebaran virus / *worm*, (5) Perusakan sistem, (6) Pemalsuan kartu kresit / *carding*, (7) Pelanggaran terhadap hak cipta, (8) Pornografi / *pornography*, (9) Penjiplakan situs / *Typosquatting*, (10) Terorisme melalui internet, (11) Pencucian uang, (12) Penipuan melalui bank / *banking fraud*, dan (13) Menggunakan jaringan orang lain tanpa hak / *phreaking*.²⁹

Sebagian pakar menganggap bahwa kejahatan mayantara (*cybercrime*) hanya modifikasi dari bentuk kejatan konvensional yang menggunakan media internet, oleh karenanya dalam penangananya hanya perlu reinterpretasi terhadap norma-norma peraturan perundang-undangan konvensional terhadap beberapa perilaku yang dianggap melawan hukum mempunyai karakteristik yang identik dengan bentuk kejahatan konvensional.³⁰ Sementara sebagian yang lainnya menganggap bahwa kejahatan mayantara merupakan kejahatan model baru yang membutuhkan aturan-aturan baru untuk mencegah atau menghukum pelakunya.

²⁷ Sutan Remy Sahdeini, *Kejahatan dan Tindak Pidana Komputer...*, hlm. 134.

²⁸ Richardus Eko Indrajit, *Konsep dan Strategi Keamanan Informasi di Dunia Cyber*, (Yogyakarta: Graha ilmu, 2014), hlm. 12-13.

²⁹ Widodo, *Hukum Pidana di bidang Teknologi Informasi ...*, hlm. 87.

³⁰ Faizin Sulisty, *Hukum Pidana dalam Perspektif ...*, hlm. 129.

C. *Defacing* Menurut Hukum Pidana Indonesia

Kejahatan dalam bahasa Inggris diistilahkan dengan *evil conduct* (perilaku jahat). Perilaku jahat tersebut dapat berupa “melakukan suatu perbuatan” (*act*) ataupun “tidak melakukan perbuatan” (*omission*). Suatu perbuatan dinilai sebagai perilaku jahat apabila perilaku tersebut dilarang atau bertentangan dengan norma yang berlaku dalam masyarakat. Sementara perilaku yang berupa “tidak melakukan sesuatu” dinilai sebagai perilaku jahat apabila menurut norma yang berlaku di masyarakat perbuatan tersebut wajib dilakukan oleh orang yang bersangkutan.³¹

Akan tetapi, kejahatan itu sendiri tidak selalu merupakan tindak pidana. Suatu kejahatan dinilai sebagai tindak pidana apabila kejahatan tersebut telah ditetapkan sebagai tindak pidana (telah dikriminalisasi) oleh suatu undang-undang pidana. Artinya, suatu tindak kejahatan hanya dapat dijatuhi sanksi pidana apabila ia telah dinyatakan sebagai tindak pidana oleh undang-undang.³² Dalam hal ini, *defacing* merupakan salah satu bentuk kejahatan dan sekaligus suatu tindak pidana sebagaimana telah diatur dalam Undang-Undang Nomor 11 Tahun 2008 tentang ITE.

Dalam undang-undang tersebut, pada Pasal 30, dinyatakan tentang perbuatan atau tindakan yang dilarang:

- (1) Setiap orang dengan sengaja dan tanpa hak atau melawan hukum mengakses komputer dan/atau Sistem Elektronik milik orang lain dengan cara apa pun.
- (2) Setiap orang dengan sengaja dan tanpa hak atau melawan hukum mengakses komputer dan/atau Sistem Elektronik dengan cara apa pun dengan tujuan untuk memperoleh informasi Elektronik dan/atau Dokumen Elektronik.
- (3) Setiap orang dengan sengaja dan tanpa hak atau melawan hukum mengakses komputer dan/atau Sistem Elektronik dengan cara apa pun dengan melanggar, menerobos, melampaui, atau menjebol sistem pengamanan.

Pasal di atas (ayat 1 sampai 3) menjelaskan tentang larangan mengakses sistem orang lain secara tidak sah. Tindakan ini dilarang karena ia merupakan langkah awal dalam kejahatan *defacing*, yakni memasuki sistem orang lain atau melakukan *hacking*.

³¹ Sutan Remy Syahdeini, *Kejahatan dan Tindak Pidana Komputer...*, hlm. 33.

³² *Ibid.*

Sementara itu, Pasal 32 ayat (1) menjelaskan lebih lanjut tentang berbagai tindakan yang masuk kategori *defecting*, yakni:

- (1) Setiap orang dengan sengaja dan tanpa hak atau melawan hukum dengan cara apa pun mengubah, menambah, mengurangi, melakukan transmisi, merusak, menghilangkan, memindahkan, menyembunyikan suatu Informasi Elektronik dan/atau Dokumen Elektronik milik Orang lain atau milik publik.

Pasal tersebut menerangkan bahwa memodifikasi terhadap suatu *website* atau masuk dalam kategori *data interference* merupakan perbuatan yang dilarang. Seperti telah dijelaskan sebelumnya bahwa *defacing* dilakukan dengan dua tahap, yakni melakukan *hacking* dan selanjutnya adalah memodifikasi *website*.

Adapun ketentuan pidana yang mengatur tentang tindak pidana kejahatan Informasi Teknologi dan Elektronik, khususnya mengenai kejahatan *defacing* yang disebutkan di atas diatur dalam UU ITE, khususnya bab XI tentang Ketentuan Pidana:

Pasal 46 dari undang-undang itu menyatakan:

- (1) Setiap orang yang memenuhi unsur sebagaimana dimaksud dalam Pasal 30 ayat (1) dipidana dengan pidana penjara paling lama 6 (enam) tahun dan/atau denda paling banyak Rp.600.000.000,00 (enam ratus juta rupiah).
- (2) Setiap orang yang memenuhi unsur sebagaimana dimaksud dalam Pasal 30 ayat (2) dipidana dengan pidana penjara paling lama 7 (tujuh) tahun dan/atau denda paling banyak Rp.700.000.000,00 (tujuh ratus juta rupiah).
- (3) Setiap orang yang memenuhi unsur sebagaimana dimaksud dalam Pasal 30 ayat (3) dipidana dengan pidana penjara paling lama 8 (delapan) tahun dan/atau denda paling banyak Rp.800.000.000,00 (delapan ratus juta rupiah).

Pasal 48 menyatakan:

- (1) Setiap Orang yang memenuhi unsur sebagaimana dimaksud dalam Pasal 32 ayat (1) dipidana dengan pidana penjara paling lama 8 (delapan) tahun dan/atau denda paling banyak Rp.2.000.000.000,00 (dua miliar rupiah).

Melihat ketentuan di atas maka tampak jelas bahwa Undang-Undang ITE telah menetapkan bentuk hukuman bagi pelaku tindak pidana *defacing*. Dengan demikian, hakim ketika hendak menjatuhkan hukuman terhadap pelaku *defacing* maka ia cukup dengan mengambil batas minimal atau batas maksimal dari jenis hukuman tersebut.

D. *Defacing* Menurut Hukum Pidana Islam

Tindak Pidana dalam hukum Islam disebut dengan istilah *jarimah*.³³ Para ulama memberikan definisi yang berbeda tentang makna kata *jarimah*. Imam al-Mawardi, misalnya, sebagaimana dikutip oleh A. Jazuli, menjelaskan pengertian *jarimah* atau perbuatan pidana sebagai berikut:

محظورات شرعية زجرا الله عنها بحد أو تعزير.

“Segala larangan *syara'* (melakukan hal-hal yang dilarang dan atau meninggalkan hal-hal yang diwajibkan) yang diancam dengan hukuman *ḥad* atau *ta'zīr*.”³⁴

Sementara Sayyid Sabiq, mendefinisikan kata *jarimah* sebagai berikut:

كل فعل محرم والفعل المحرم كل فعل خطره الشارع ومنع منه لما فيه من ضرر وقع على الدين والنفس أو الفعل أو العرض أو المال.

“Setiap perbuatan yang dilarang oleh hukum *syara'* untuk melakukannya. Perbuatan yang dilarang adalah semua kegiatan yang dilarang oleh *syara'* yang apabila dilanggar maka akibatnya akan membahayakan terhadap agama, jiwa, kehormatan, dan harta benda.”³⁵

Dari beberapa definisi tentang *jarimah* sebagaimana dijelaskan di depan, maka dapat diambil kesimpulan bahwa *jarimah* adalah suatu tindakan yang bertentangan dengan ketentuan hukum *syara'*, yang bagi pelakunya akan dikenai hukuman *ḥad* atau *ta'zīr*.

³³ Itilah *jarimah* berasal dari kata *jarama*, yang berarti berbuat dosa, berbuat salah, atau berbuat jahat. Pelaku atau orang yang melakukan perbuatan dosa tersebut dinamakan *jarimun*, sedangkan orang yang dikenai perbuatan itu disebut *majrām alaib*.

³⁴ A. Jazuli, *Hukum Pidana Islam Upaya Menanggulangi Kejahatan dalam Islam*, cet. II (Jakarta: Raja Grafindo Persada, 1997), hlm. 11.

³⁵ Sayyid Sabiq, (terj) *Fiqih Sunnah X*, (Bandung: Al-Ma'arif, 1997), hlm. 11.

Dalam hukum Pidana Islam, perbuatan atau tindak pidana (*jarīmah*) itu sendiri dikelompokkan ke dalam beberapa kategori:³⁶

1. *Jarīmah Hudūd*, yakni tindak pidana yang sanksi atau hukumannya telah ditetapkan oleh Allah secara langsung, sebagaimana dapat disimak dalam Al-Qurān maupun sunnah Nabi.

Jumhur ulama' memasukkan tujuh tindak pidana yang masuk kategori *jarīmah hudūd*, yakni: (a) zina, (b) *qozaf* (tuduhan palsu zina), (c) *sariqah* (pencurian), (d) *hirābah* (perampokan), (e) *riddah* (murtad), (f) *al-baghy* (pemberontakan), dan (g) *syurb al-khamr* (meminum khamr).

2. *Jarīmah Qiṣās Diyāt*, yaitu kejahatan terhadap jiwa (membunuh) dan anggota badan (pelukaan) yang diancam dengan hukuman *qiṣās* (serupa) atau *diyāt* (ganti rugi pelaku kepada pihak korban).

Dalam hukum pidana Islam yang termasuk *qiṣās diyāt* adalah (a) pembunuhan dengan sengaja (b) pembunuhan semi sengaja (c) tindakan yang menyebabkan seseorang meninggal dikarenakan kealpaan atau kesalahan (d) penganiayaan dengan sengaja, dan (e) tindakan yang menyebabkan orang terluka karena kealpaan atau kesalahan.³⁷

3. *Jarīmah Ta'zīr*, yaitu hukuman yang ditetapkan atas perbuatan maksiat atau jinayah yang tidak dikarenakan *ḥad* dan *kafarat*.³⁸

Terkait dengan *jarīmah ta'zīr*, Abdul Qadir Awdah sebagaimana dikutip oleh Makhrus Munajat, mengelompokkannya ke dalam tiga (3) bagian, yaitu:

- a. *Jarīmah hudūd* dan *qiṣās diyāt* yang mengandung unsur *subhat* atau tidak memenuhi syarat, namun hal itu sudah dianggap sebagai perbuatan maksiat, seperti *watī'* subhat, pencurian harta *syirkah*, pembunuhan ayah terhadap anaknya, dan pencurian yang bukan harta benda.
- b. *Jarīmah ta'zīr* yang jenis tindak pidana yang ditentukan oleh *naṣ*, tetapi sanksinya diserahkan kepada penguasa, seperti sumpah

³⁶ Makhrus Munajat, *Hukum Pidana Islam (Fiqh Jinayat)*, (Yogyakarta: Pesantren Nawasea Press, 2010), hlm. 105.

³⁷ *Ibid.*, hlm. 135.

³⁸ *Ibid.*, hlm. 145. Secara bahasa, *ta'zīr* berarti mencegah dan menolak. Hukuman *ta'zīr* dimaksudkan untuk member efek jera pada pelaku supaya tidak mengulangi perbuatannya.

palsu, saksi palsu, mengurangi timbangan, menipu, mengingkari janji, mengkhianati amanat, dan menghina agama.

- c. *Jarīmah ta'zīr* yakni jenis kejahatan yang pemberian sanksinya secara penuh menjadi wewenang penguasa demi terealisasinya kemaslahatan umat. Dalam hal ini, unsur akhlak menjadi pertimbangan yang paling utama. Misalnya pelanggaran terhadap peraturan lingkungan hidup, lalu lintas, dan pelanggaran terhadap peraturan lainnya.³⁹

Suatu perbuatan dikatakan sebagai tindak pidana (*jarīmah*) dan diberikan sanksi adalah apabila tindakan tersebut telah memenuhi unsur-unsur yang melekat pada tindakan pidana. Unsur-unsur ini ada yang bersifat umum dan ada yang khusus. Unsur umum berlaku untuk semua bentuk *jarīmah*, sedangkan unsur khusus hanya berlaku untuk masing-masing *jarīmah* dan berbeda antara *jarīmah* yang satu dengan yang lain. Menurut Abdul Qadir Audah, sebagaimana dikutip oleh Makhrus Munajat, ada tiga hal yang termasuk kategori unsur umum dari *jarīmah*, yaitu:

- a. Unsur formal, yaitu adanya *nash* atau ketentuan yang menunjukkan bahwa tindakan tersebut merupakan *jarīmah*.
- b. Unsur materiil, yaitu adanya perbuatan melawan hukum yang benar-benar dilakukan.
- c. Unsur moril, yaitu niat pelaku untuk berbuat *jarīmah*. Unsur ini menyangkut tanggung jawab pidana yang akan dikenakan atas orang yang telah *baligh*, sehat akal, dan *ikhtiyar* (kebebasan berbuat).⁴⁰

Sedangkan unsur-unsur khusus dalam *jarīmah* adalah:

- a. Unsur niat, yakni adanya niat untuk melakukan *jarīmah*.
- b. Permulaan pelaksanaan.
- c. Tidak selesainya perbuatan karena kehendaknya sendiri

Unsur-unsur tersebut, baik yang bersifat umum maupun yang khusus, harus terdapat pada suatu perbuatan untuk bisa digolongkan dalam *jarīmah* dan dapat dijatuhi hukuman.

Tidak pidana *defacing* jika dilihat dalam perspektif hukum pidana

³⁹ Makhrus Munajat, *Reaktualisasi Pemikiran Hukum Pidana Islam*, (Yogyakarta: Cakrawala, 2006), hlm. 13.

⁴⁰ *Ibid.*

Islam maka bisa dikategorikan sebagai *jarimah ta'zir*, karena ketentuan dan sanksinya belum ada dalam *nash* Al-Qur'an maupun sunnah nabi dan pemberian sanksinya diserahkan sepenuhnya kepada penguasa atau hakim.⁴¹ Selain itu, *defacing* juga tidak bisa diqiyaskan dengan *jarimah hudud* karena tidak ada 'illat hukum yang sama.⁴²

Dalam kaitannya dengan *defacing* yang bisa dikategorikan sebagai *jarimah ta'zir*, maka hukuman atau sanksinya adalah hukuman *ta'zir*. Dalam hal ini, Islam memberi kewenangan penuh kepada *ulil amri* untuk menentukan jenis dan kadar beratnya hukuman *ta'zir*.⁴³

Adapun bentuk hukuman *ta'zir* itu sendiri banyak macamnya, mulai dari yang paling berat hingga yang paling ringan. Dalam hal ini hakim diberi wewenang untuk memilih jenis hukuman di antara hukuman-hukuman tersebut sesuai dengan kejahatan yang dilakukan. Bentuk-bentuk hukuman *ta'zir* itu, di antaranya, adalah (1) hukuman mati, (2) hukuman jilid, (3) hukuman-kawalan (penjara kurungan), (4) hukuman salib, (5) hukuman ancaman (*tahdid*), teguran (*tanbih*) dan peringatan, (6) hukuman pengucilan (*al hajru*), dan (8) hukuman denda (*tahdid*):⁴⁴

Penetapan hukuman *ta'zir* terhadap suatu kejahatan harus sesuai dengan kemaslahatan, sebagaimana kaidah beriku: *at-Ta'zir yaduru ma'a al-mashlahah* (*ta'zir* itu tergantung pada tuntutan kemaslahatan). Oleh karena itu, seorang hakim yang akan menjatuhkan hukuman *ta'zir* haruslah mencermati betul tindak kejahatannya, serta mempertimbangkan situasi dan kondisi yang melingkupinya, baik yang menyangkut pelaku, korban, waktu, dan tempatnya. Demikian juga hak terdakwa dan hak korban harus dipertimbangkan secara seimbang.⁴⁵

⁴¹ M. Nurul Irfan dan Masyrofah, *Fiqh Jinayat*, cet. I (Jakarta: Amzah, 2013), hlm. 188.

⁴² Wahbah Zuhaili, sebagaimana dikutip oleh Makhrus Munajat, mendefinisikan *ta'zir* sebagai: "hukuman yang ditetapkan atas perbuatan maksiat atau jinayah yang tidak dikenakan *had* dan tidak pula *kifarat*." Makhrus Munajat, *Hukum Pidana di Indonesia...*, hlm. 178.

⁴³ Mustofa Hasan dan Beni Ahmad Saebani, *Hukum Pidana Islam Fiqh Jinayah*, (Bandung: Pustaka Setia, 2013), hlm. 27.

⁴⁴ *Ibid.*, hlm. 595-596.

⁴⁵ A. Djazuli, *Fiqh Jinayah* ..., hlm. 241.

E. Penutup

Defecting merupakan salah satu bentuk kejahatan dunia maya yang dilakukan oleh orang-orang yang tidak bertanggung jawab dan telah banyak yang menjadi korbannya. Untuk menghindari dan mencegah semakin berkembangnya kejahatan di dunia maya dan untuk melindungi masyarakat, maka pemerintah Indonesia pada tahun 2008 telah membuat aturan hukum dalam bentuk undang-undang, yakni Undang-Undang Nomor 11 Tahun 2008 tentang ITE (Informasi Teknologi dan Elektronik). Dalam undang-undang tersebut, kejahatan *defecting* diatur dalam beberapa Pasal, di antaranya Pasal 30 dan 32 yang menjelaskan tentang makna dan cakupan *defecting*, dan Pasal 46 dan 48 yang mengatur tentang bentuk hukuman pidana bagi pelaku *defecting*.

Dalam hukum Pidana Islam (*fiqih jinayah*), *defecting* bisa dikategorikan sebagai *jarimah ta'zir*, yakni suatu bentuk kejahatan yang sanksi hukumnya tidak disebutkan secara langsung oleh *nash* Al-Qur'an dan as-Sunnah. Oleh karena itu, sanksi atau hukuman bagi pelaku *jarimah ta'zir* ini ditentukan oleh penguasa atau hakim. Dalam hal ini hakim memiliki kekuasaan penuh untuk menjatuhkan hukuman bagi pelaku *jarimah ta'zir* sesuai dengan kadar kejahatan yang dilakukannya. Meski demikian, hukuman tersebut harus senantiasa didasarkan pada upaya untuk mewujudkan keadilan serta dalam kerangka menciptakan kemaslahatan bersama.

Secara substansi, kebijakan hukuman dalam hukum pidana Indonesia dan *fiqih jinayah* (hukum pidana Islam) mempunyai semangat dan tujuan yang sama, yaitu upaya melakukan pencegahan dan penangkalan terhadap semua bentuk kejahatan, termasuk kejahatan *defecting*, agar tidak semakin menyebar dan berkembang secara luas. Kedua sistem hukum tersebut juga sama-sama bertujuan menciptakan keadilan dan kebaikan (kemaslahatan) bagi sesama manusia. Selain itu, hukuman di dalam kedua sistem hukum tersebut juga tersimpan semangat (tujuan) untuk memberikan efek jera kepada pelaku kejahatan. Dengan demikian, perilaku atau tindak kejahatan diharapkan akan bisa diminimalisir.

DAFTAR PUSTAKA

- Hanafi, Ahmad, *Azaz-azaz Hukum Pidana Islam*, Jakarta: Bulan Bintang, 2002.
- Hasan, Mustofa dan Beni Ahmad Saebani, *Hukum Pidana Islam - Fiqh Jinayah*, Bandung: Pustaka Setia, 2013.
- Indrajit, Richardus Eko, *Konsep dan Strategi Keamanan Informasi di Dunia Cyber*, Yogyakarta: Graha ilmu, 2014.
- Irfan, M. Nurul dan Masyrofah, *Fiqh Jinayat*, cet. I, Jakarta: Amzah, 2013.
- Jazuli, A., *Hukum Pidana Islam - Upaya Menanggulangi Kejahatan dalam Islam*, cet. II, Jakarta: Raja Grafindo Persada, 1997.
- Mansur, Dikdik M. Arief dan Elisatris Gultom, *Cyberlaw: Aspek Hukum Teknologi Informasi*, cet. II Bandung: Refika Aditama, 2009.
- Munajat, Makhrus, *Reaktualisasi Pemikiran Hukum Pidana Islam*, Yogyakarta: Cakrawala, 2006.
- _____, *Hukum Pidana Islam di Indonesia*, Yogyakarta: Teras, 2009.
- _____, *Hukum Pidana Islam (Fiqh Jinayat)*, Yogyakarta: Pesantren Nawasea Press, 2010.
- Muslich, Ahmad Wardi, *Hukum Pidana Islam*, cet. II, Jakarta: Sinar Grafika, 2005.
- Riswandi, Budi Agus, *Hukum Internet di Indonesia*, Yogyakarta: UII Press, 2003.
- Sabiq, Sayyid, (terj) *Fiqh Sunnah X*, Bandung: Al-Ma'arif, 1997.
- Sulistyo, Faizin, *Hukum Pidana dalam Perspektif*, Denpasar: Pustaka Larasan, 2012.
- Syahdeini, Sutan Remi, *Kejahatan dan Tindak Pidana Komputer*, Jakarta: Pustaka Utama Grafiti, 2009.
- Tahir, Achmad, *Cybercrime (Akar Masalah, Solusi, dan Penanggulangannya)*, Yogyakarta: Suka Press, 2011.

Wahid, Abdul dan Mohammad Labib, *Kejahatan Mayantara (Cybercrime)*, Jakarta: Refika Aditama, 2005.

Widodo, *Aspek Hukum Pidana Kejahatan Mayantara*. Yogyakarta: Aswaja Pressindo. 2013.

_____, *Memerangi Cybercrime Karakteristik Motivasi dan Strategi Penanganannya dalam Perspektif Kriminologi*. Yogyakarta: Aswaja Pressindo. 2013.